STATE of ARIZONA

Arizona **D**epartment **O**f **A**dministration	**Agency** **STANDARD** **P800-T2-S01** **Rev. 0**	**TITLE: Access Control** **Effective Date: January 31, 2009**

1. AUTHORITY

1.1. The authority for this Standard is based on Arizona Revised Statute 41-703 and the ADOA Policy A800 – Information Security Policy.

2. PURPOSE

2.1. The purpose of this Standard is to establish the responsibilities and restrictions to be complied with by all users of ADOA information resources.

3. SCOPE

3.1. This Standard applies to all ADOA employees, contractors and other entities using ADOA information resources.

3.2. The ADOA Director, in conjunction with the ADOA Chief Information Officer (CIO) and the ADOA Information Security (AIS) Manager, is responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies and Standards.

4. DEFINITIONS AND ABBREVIATIONS

4.1. **ADOA –** Arizona Department of Administration

4.2. **AIS** – ADOA Information Security

4.3. **AIS Manager –** ADOA Information Security Manager

4.4. **Access Control:** A mechanism that can grant or restrict the use of information resources and provide reasonable assurance that information resources are protected against unauthorized modification, disclosure, loss or misuse.

4.5. **Account Management: P**rocedures directing the steps and timing for reviewing, granting and/or withdrawing information resource access privileges.

4.6. **Account Provisioning:** Procedures directing the steps and requirements for creating user accounts and granting information resource access privileges.

4.7. **Information Flow:** The flow of data into and out of an ADOA information resource, including the processes that occur to input or output data in an ADOA information resource.

4.8. **Information Resource:** Any computing device, peripheral, software, local and wide area networks (LAN and WAN), communications equipment, (including fax machines and telephones), communications software (including the Internet, Intranet and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities and data distribution, electronic data or related consumable (e.g. paper, disk space, central processor time, network bandwidth) information and data owned or controlled by ADOA.

4.9. **Special Access Privileges:** high-level privileges (such as root access on distributed systems), that provide access to sensitive network devices, operating system files and/or settings, or high level software application capabilities.

4.10. **System Administrator:** Person(s) designated to manage and maintain an information resource.

4.11. **System Owner:** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information resource.

5. STANDARD

5.1. Account Provisioning

5.1.4. All ADOA information resource authorized users must have an individually owned, unique account and a secure password in order to be authenticated to an ADOA information resource.

5.1.5. Passwords will meet requirements of Statewide Standard P800-S820, Authentication and Directory Services, unless otherwise prevented by the capabilities of the information resource.

5.1.6. Authorized user account requests, access/rights changes and account deletions are only accepted from the user’s manager or system security administrator and must be made via the proper request form.

5.1.7. All authorized users must complete required security awareness training, sign a non-disclosure agreement and sign an acknowledgement of their responsibilities for Acceptable Use of ADOA information resources prior to accessing ADOA information resources.

5.1.8. Accountability for actions taken on an ADOA information resource belongs to the owner of the UserID under which those actions take place.

5.1.9. User authorization should be based on least privilege required to perform assigned tasks and permissions, or rights, shall only be granted in accordance with the requestor’s group or role membership(s).

5.1.10. A request for an account with special access privileges must be received from a user’s manager and must include documentation specifying the purpose of the extended privileges.

5.2. **Account Management**

5.2.4. System administrators shall take reasonable measures to ensure that all accounts belong to currently authorized users. Accounts must be kept current through the timely addition of new accounts and the deletion of expired accounts. Events requiring action include the following and apply to divisional employees and contractors:

a. New hire

b. Transfer to another agency

c. Change of duties

d. Resignation

e. Termination

f. Report of inappropriate behavior as defined by the acceptable use form and non-disclosure agreement

5.2.5. Thresholds for acceptable periods of inactivity for user accounts shall be documented and monitored according to system categorization. Inactive accounts meeting the determined thresholds shall be initially disabled and subsequently removed.

5.2.6. System Administrators shall ensure access controls are applied to accounts through either login scripts and/or access rights that limit access to authorized and required areas only (least privilege required to perform assigned tasks).

5.2.7. System administrators, in conjunction with system owners, must perform regular reviews of user and administrator accounts with special privileges that have access to view and/or modify sensitive or significant data to ensure access levels are appropriate for their position requirements.

5.2.8. Access logs, if available, will be enabled and protected from accidental or deliberate overwriting. Access logs should be proactively analyzed, correlated with other logs and evaluated. Systems should be configured to log information locally and then sent to a remote system. Logs should contain details of:

a. Access by types of user

b. Servicing activities

c. Failed sign-on attempts

d. Error/exception conditions

e. Sufficient information to identify individual userIDs, resources and information accessed, access paths, and patterns of access

5.2.9. User accounts will be locked from further use following a maximum of three detected, unsuccessful login attempts. ADOA password resetting procedures will ensure that the correct account holder is requesting the reset.

5.2.10. Procedures to address requirements for issuing new passwords to replace forgotten passwords shall be documented and maintained.

5.2.11. Access to information, resources and services will be in accordance with Statewide Standard P800-S885, IT Physical Security, Statewide Standard P800-S2890, Personnel Security, and Statewide Standard P800-S810, Account Management. Internal and external connectivity to networks to provide access to resources and services will be in accordance with Statewide Standard P800-S830, Network Security.

5.2.12. Where reasonably and economically feasible, the ADOA employee or contractor in charge of security for a “like” group of information resources or services should not be responsible for the security of other groups. For example, the individual establishing user accounts should not be the same individual that grants access to software applications and associated databases.

6. STANDARD NON-COMPLIANCE

6.1. All authorized users of ADOA Information Resources are responsible for understanding and adhering to this standard.

6.2. For non-compliance with this standard, all ADOA employees shall be subject to Human Resource progressive discipline, with the understood exception, that management may choose to take appropriate action commensurate with the seriousness of the offense.

6.3. Contractors and other authorized users will be held to contractual agreements.

7. REFERENCES

7.1. Arizona Revised Statute 41-703

7.2. ADOA Policy A800 – IT Security

7.3. ADOA Standard A800-O1-S01 – Personnel Security

7.4. Statewide Standard P800-S810 – Account Management

7.5. Statewide Standard P800-S820 – Authentication and Directory Services

7.6. Statewide Standard P800-S885 – IT Physical Security

7.7. Statewide Standard P800-S830 – Network Security

8. ATTACHMENTS

8.1. No attachments accompany this standard.